Arion 3001-4
Router and Firewall
User's Manual

Rev 1.0
Mar 2004

Table of Contents

1. INTRODUCTION 1

1.1. PRODUCT OVERVIEW 1

2. HARDWARE DESCRIPTION 2

2.1. FRONT PANEL 2

Arion 3001-4 – Front Panel 2

2.2. REAR PANEL 3

Arion 3001-4 Rear Panel 3

3. DEFAULT VALUES 4

3.1. PASSWORD 4

3.2. DEFAULT NETWORK SETUP 4

3.3. OTHER DEFAULT SETUP 4

4. CONFIGURING YOUR ARION 3001-4 – LOGIN 5

5. CONFIGURING YOUR ARION 3001-4 – GENERAL SETUP 6

5.1. SYSTEM 6

5.1.1. Time Zone 6

5.1.2. Password Settings 6

5.1.3. Remote Management 7

5.2. WAN SETTINGS 8

5.2.1. Dynamic IP 8

5.2.2. PPPoE 8

5.2.3. Static IP 9

5.2.4. DNS 10

5.3. LAN SETTINGS 11

5.4. NAT SETTINGS 12

5.4.1. Address Mapping 12

5.4.2. Virtual Server 12

5.4.3. Special Application 13

5.5. FIREWALL 15

5.5.1. Access Control 15

5.5.2. URL Blocking 17

5.5.3. Schedule Rule 18

5.5.4. Intrusion Detection 19

5.5.5. DMZ 21

6. UPNP 22

7. DDNS 23

8. TOOLS 24

8.1. CONFIGURATION TOOLS 24

8.2. FIRMWARE UPGRADE 24

8.3. RESET 24

9. STATUS 26

9.1. INTERNET CONNECTION 26

9.2. DEVICE STATUS 27

9.3. SECURITY LOG 27
9.4. DHCP CLIENT LOG 28
9.5. VOIP STATUS 28
GLOSSARY 29

1. Introduction

The Arion 3001-4 is an Integrated Access Device that combines a Voice Gateway and a Broadband Router in a single device. The Broadband router is designed to share a single Internet Access among two or more PCs in a household and to provide Internet security for the PCs connected to its LAN ports. The Arion 3001-4 also provides voice over IP (VoIP) functionality that enables you to make voice calls over the Internet. The Arion 3001-4's simple installation and setup can be used by a wide range of people, while providing networking professionals with easy to configure advanced features. Please read this Router/Firewall User Guide for advanced features of this product.

With Arion 3001-4, ATIU can deliver Voice services over high-speed internet access as well as an interface unit that will allow you to connect multiple PCs or other IP devices in a cost effective manner.

1.1. Product Overview

The Arion 3001-4 is an Integrated Access Devices (IAD) equipped with one standard analog telephone port, one WAN Fast Ethernet 10/100BaseTX port and four LAN Fast Ethernet 10/100BaseTX ports.

By transporting voice signal over the Internet connection, the Arion 3001-4 offers the residential customer a second line without the need for the second subscriber copper loop. It also has the ability to route data between multiple user PCs on the LAN side to/from the Internet. The Arion 3001-4 is H.323 v2 compliant for Voice over IP (VoIP) and it is compatible with Cable and ADSL Broadband Internet Service with built-in DHCP and PPPoE client.
The services offered to the internal network are:

- DHCP Server,
- Network Address Translation (NAT),
- Network Address Port Translation (NAPT) and
- IPSEC pass through.

The Arion 3001-4 has the ability to prioritize voice over data through IP Layer QoS, Ethernet Layer CoS (Classes of Service) and VLAN Tagging. It also supports voice compression (G.723.1 and G.729 AB voice CODECs), echo cancellation, dynamic jitter buffer, silence suppression and comfort noise generation.

The Arion 3001-4 also has 8 LEDs on the front panel that provide status indication and can be for troubleshooting purposes. See section 2.1

2. Hardware Description
2.1. Front Panel

Arion 3001-4 – Front Panel

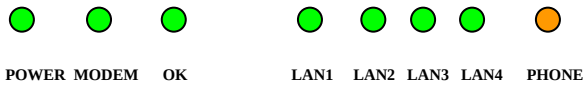

Figure 2-1

Function	Label	Display Color	Meaning
Power	POWER	Light (Green)	Power on, normal operation
		Blink	Firmware loading
		Off	Power off or failure
WAN	MODEM	WAN Light (Green)	Green Link /Active : WAN Connection is OK
		WAN Blink (Green)	Link /Active : data transmitting or receiving
		Off	Link /Active : connection is not established
Internet Link	OK	Light (Green)	Internet connection is OK
		Off	Internet connection is failed
LAN	LAN1 LAN2 LAN3 LAN4	Light (Green)	Link /Active : Connection is OK
		Blink	Link /Active : data transmitting or receiving
		Off	Link /Active : connection is not established
Phone	PHONE	Light (Orange)	Off hook
		Blink(Ring)	Ring for Incoming call (follow the ring pattern)
		Blink(Alert)	Gatekeeper register failed(One second on, One second off)
		Off	On hook

Table 2-1

2.2. Rear Panel

Arion 3001-4 Rear Panel

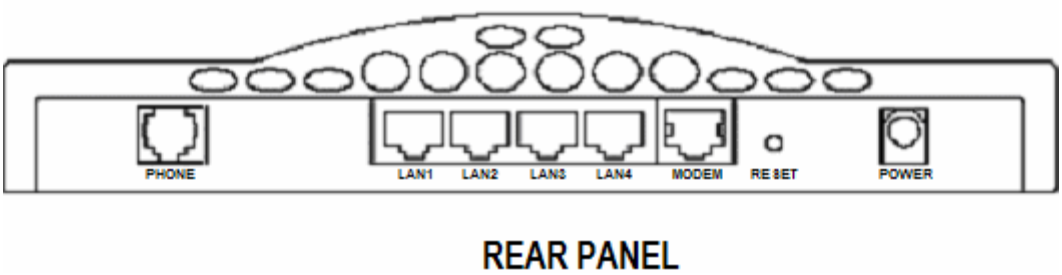

Figure 2-2

Item	Connector	Function
1	**Phone**	Connect to Phone set。
2	**LAN (1-4)**	4 port (10/100Mbps) RJ-45 connector, connect to PC or local switch/hub.
3	**MODEM**	Connect to Cable or ADSL Modem 。
4	**RESET (Reboot)**	Reset button. Press for one second to reset the device or press for 5 seconds to reset to the factory default.
5	**12V DC**	Power connector.

Table 2-2

3. Default Values

3.1. Password

The default user name/password is user/user. For security and management reasons, we recommend that you set up a new password after you first login to the system. Once you have changed the password, it is important that you write it down and keep this information in a safe location. If you happen to forget the user name / password, you can push and hold the reset button for at least 5 seconds, until all of the LEDs flash; your Arion 3001-4 now be reset to factory default.

3.2. Default Network setup

LAN Setup		WAN Setup
IP Address	192.168.1.1	DHCP Client enabled
Subnet Mask	255.255.255.0	
DHCP server	Enable	
DHCP IP range	100 IP addresses from 192.168.1.100 to 192.168.1.199	

Table 3-1

3.3. Other Default setup

Time Zone	Eastern Standard Time
Firewall	Off
UPnP	Off
DDNS	Off

Table 3-2

4. Configuring Your Arion 3001-4 – Login

Now that you have successfully connected your computer to the Internet and activated your voice service, you will need to login into the Arion 3001-4 to configure it for your LAN.

1. Open your Web browser (i.e., Internet Explorer or Netscape Navigator).

2. In the "Address" field type "http://192.168.1.1" and press <ENTER>.

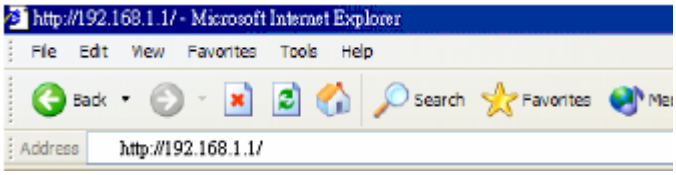

Figure 4-1

3. The Arion 3001-4 login screen will appear. The default User name/Password setting is user/user. For security reasons, you should assign a new password as soon as possible. **Note.** The password login in case sensitive.

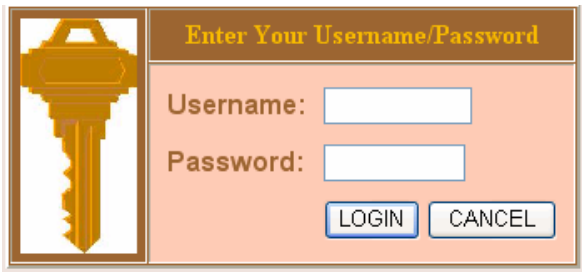

Figure 4-2

4. Once you have logged in successfully, the first page will appear as below:

General Setup
This IAD supports advanced Router and VoIP Gateway functions. You can use these pages to configure the WAN/LAN, firwall, NAT setting.

Figure 4-3

5. Configuring Your Arion 3001-4 – General Setup

5.1. System

5.1.1. Time Zone

Set the proper time zone and the configure time server for the Arion 3001-4. The default time zone is "Eastern Standard Time, Toronto, Canada".

When you enable the Automatic Time Server Maintenance option you will need to configure two timeservers, see example provided below.

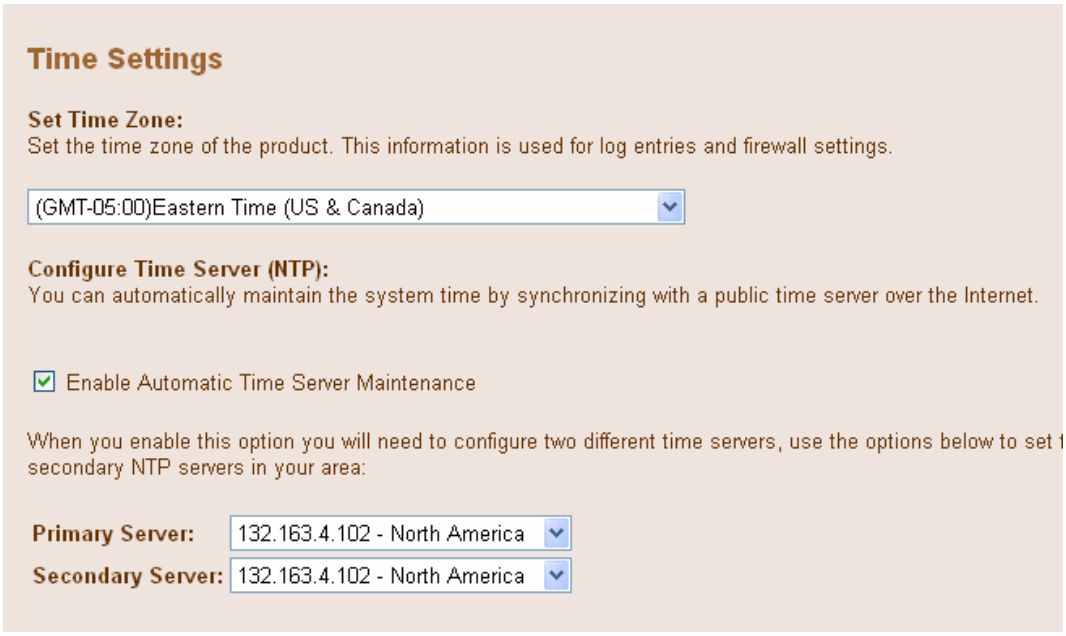
Time Settings
Set Time Zone:
Set the time zone of the product. This information is used for log entries and firewall settings.
(GMT-05:00)Eastern Time (US & Canada)
Configure Time Server (NTP):
You can automatically maintain the system time by synchronizing with a public time server over the Internet.
Enable Automatic Time Server Maintenance
When you enable this option you will need to configure two different time servers, use the options below to set t
secondary NTP servers in your area:
Primary Server:
132.163.4.102 - North America
Secondary Server:
132.163.4.102 - North America

Figure 5-1

5.1.2. Password Settings

Set the password of the user. The Idle Time Out value is used for Arion 3001-4 to log out automatically when no access to the web after this timeout value. The default Idle Time out value is 10 minutes.

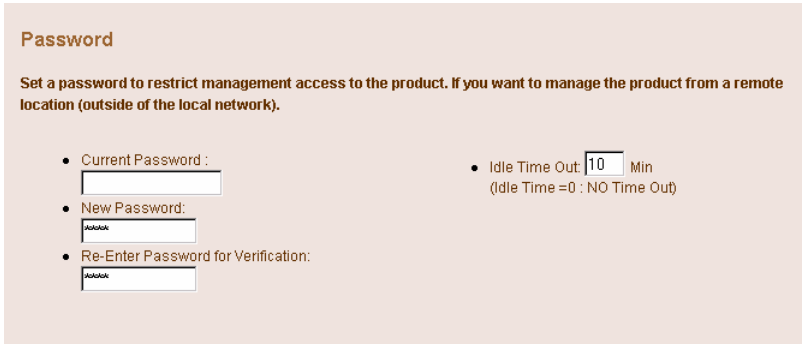
Password
Set a password to restrict management access to the product. If you want to manage the product from a remote location (outside of the local network).
Current Password :
New Password:
Re-Enter Password for Verification:
Idle Time Out: 10 Min
(Idle Time =0 : NO Time Out)

Figure 5-2

5.1.3. Remote Management

The "Remote Management" feature can restrict the access to your Arion 3001-4 from the Internet. Unless you have a need to access Arion 3001-4 from outside your home, this feature should be disabled. You can enable it from a specific IP address or from any outside IP address. The IP setting of "0.0.0.0" allows any person from any IP address to login into the device. When the 'Enabled" is not checked, the remote login feature will be disabled. The default setting is that Enable is not checked.

Figure 5-3

The remote user can login using WAN IP. The default port number is 8080. For example, if your public IP address is 211.20.16.1, then you would type the following string into your browser to remotely access your Arion 3001-4.

Figure 5-4

5.2. WAN Settings

The Arion 3001-4 supports 3 types of WAN connection – Dynamic IP (DHCP Client), PPPoE, and Static IP.

5.2.1. Dynamic IP

This mode allows the Arion 3001-4 to enable its DHCP client to get an IP address from your high-speed service provider. The Host Name is optional, but may be required by some high-speed Service Providers. The default MAC address is set to the WAN's physical interface on the Arion 3001-4. If required by your high-speed Service Provider, you can use the <Clone MAC Address> button to copy the MAC address of the Network Interface Card installed in your PC and replace the WAN MAC address with this MAC address. If necessary, you can reach restore the MAC address to the factory setting <See Section 8.1>.

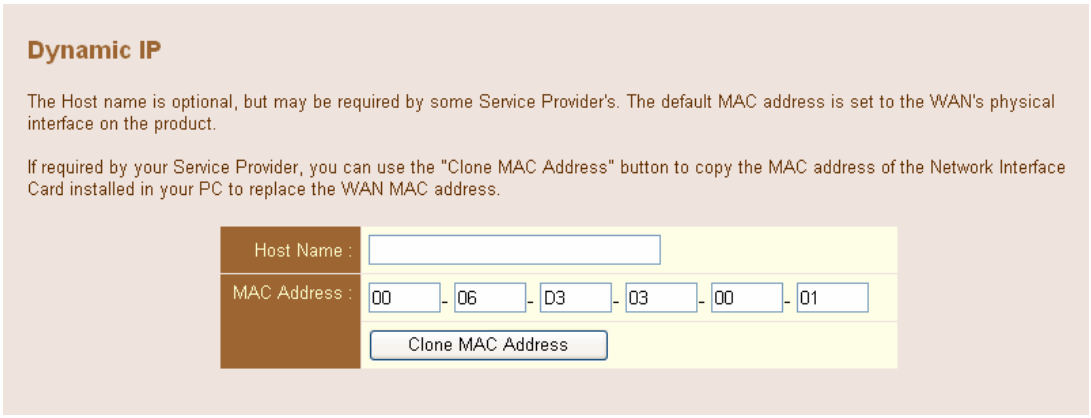
Dynamic IP
The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the product.
If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.
Host Name :
MAC Address :
00 - 06 - D3 - 03 - 00 - 01
Clone MAC Address

Figure 5-5

5.2.2. PPPoE

This mode allows the Arion 3001-4 to act as a PPPoE client. You will be required to enter the PPPoE user name and password originally provided by your high-speed Service Provider. The Service Name is normally optional; some high-speed service providers may require it. Enter a Maximum Idle Time (in seconds) to define a maximum period of time for which the Internet connection is maintained during periods of inactivity. If the connection is inactive for longer than the Maximum Idle Time, then the connection to your high-speed provider will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet. The default is Maximum Idle Time of 0 (Zero) and Auto Reconnect is enabled. This setting is required to enable incoming VoIP calls to complete.

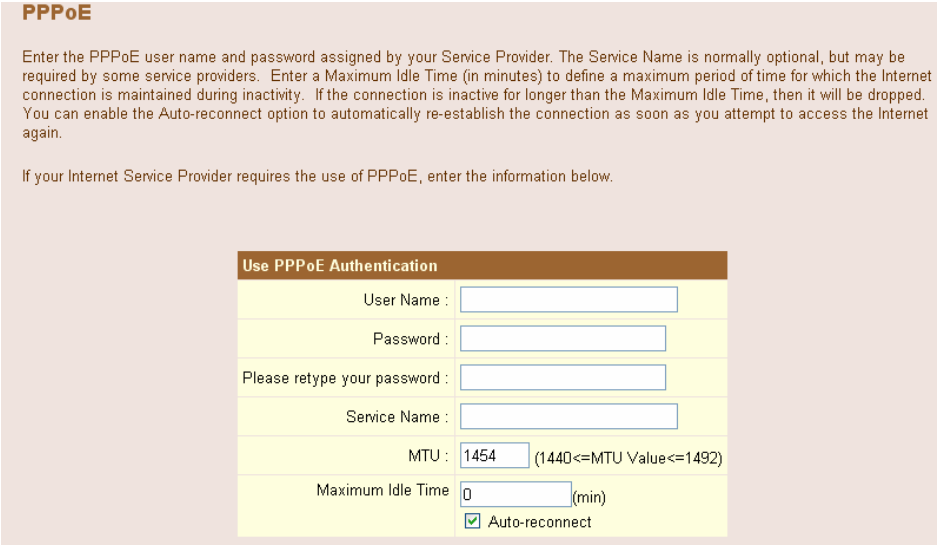
PPPoE
Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.
If your Internet Service Provider requires the use of PPPoE, enter the information below.
Use PPPoE Authentication
User Name :
Password :
Please retype your password :
Service Name :
MTU : 1454 (1440<=MTU Value<=1492)
Maximum Idle Time 0 (min)
Auto-reconnect

Figure 5-6

5.2.3. Static IP

If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided.

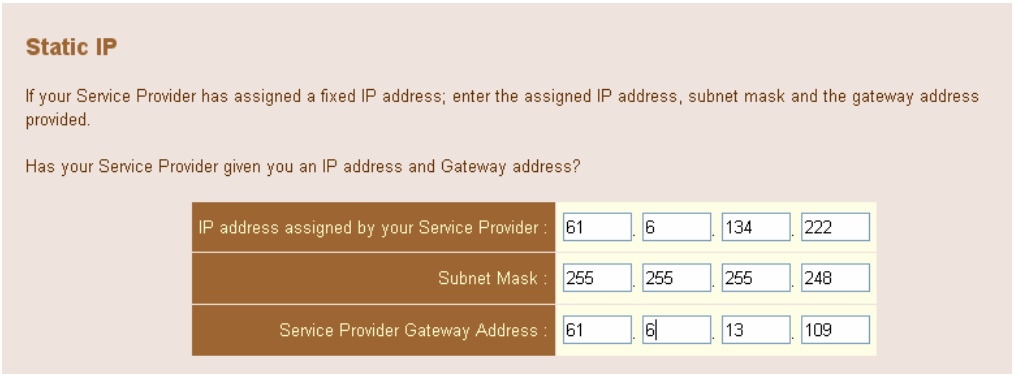
Static IP
If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided.
Has your Service Provider given you an IP address and Gateway address?
IP address assigned by your Service Provider : 61 . 6 . 134 . 222
Subnet Mask : 255 . 255 . 255 . 248
Service Provider Gateway Address : 61 . 6 . 13 . 109

Figure 5-7

5.2.4. DNS

Most service providers provide a DNS server via DHCP or PPPoE for speed and convenience. If you have a static IP address, or if there is a DNS server that you would rather use, you need to specify the primary and secondary IP address here. When primary DNS does not work, system will automatically use secondary DNS.

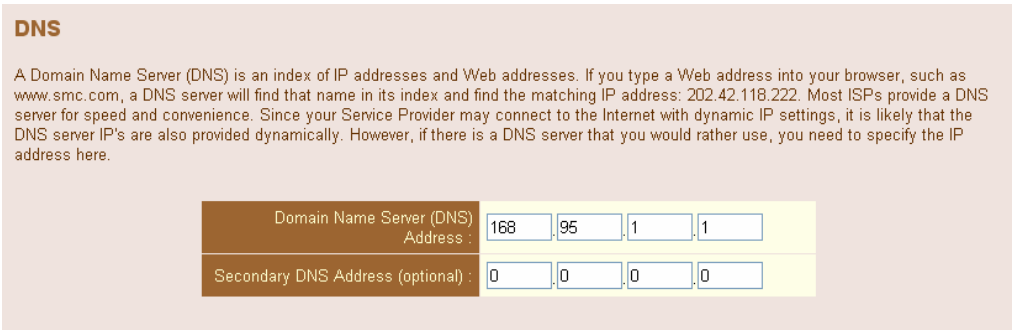
DNS
A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 202.42.118.222. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.
Domain Name Server (DNS) Address :
168 95 1 1
Secondary DNS Address (optional) :
0 0 0 0

Figure 5-8

5.3. LAN Settings

You can enable DHCP to dynamically allocate IP addresses to each of your PCs connected to the Arion 3001-4. When DHCP server is enabled, you need to enter the IP address range for the local hosts. The default range is 192.168.1.100 through 192.168.1.199.

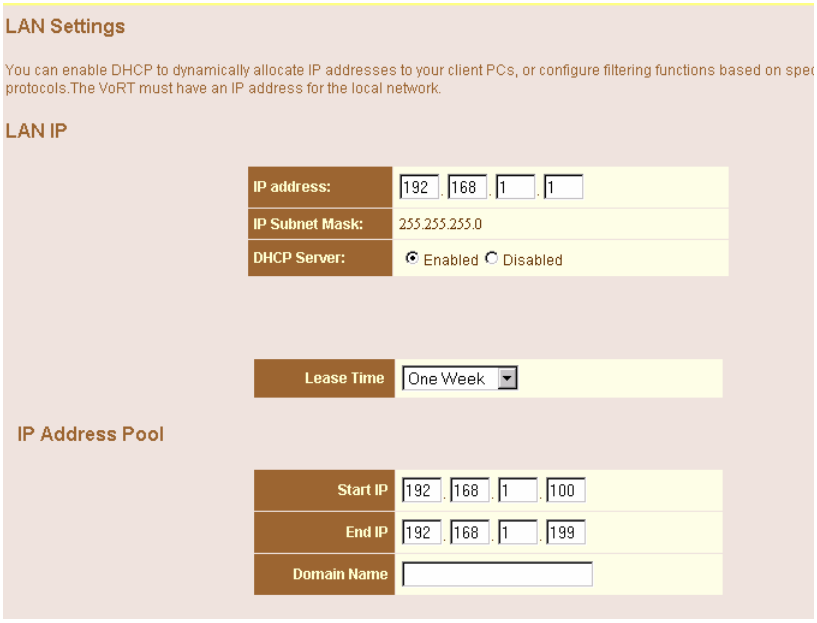
LAN Settings
You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on spec
protocols.The VoRT must have an IP address for the local network.
LAN IP
IP address:
192 . 168 . 1 . 1
IP Subnet Mask:
255.255.255.0
DHCP Server:
Enabled Disabled
Lease Time
One Week
IP Address Pool
Start IP
192 . 168 . 1 . 100
End IP
192 . 168 . 1 . 199
Domain Name

Figure 5-9

The domain name field is empty in most case. In some special ISP need input domain name field.

5.4. NAT Settings

5.4.1. Address Mapping

Arion 3001-4 supports multiple public IP addresses. It allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This page allows you to enter up to 10 address mappings between a set of private IP addresses and one global IP address. After these settings have been completed, the Arion 3001-4 will map the set of private IP addresses to the global IP address when accessing to the Internet. This could be useful in the gaming and some particular multimedia applications; however most users have only one public address and will use only the first mapping on this page.

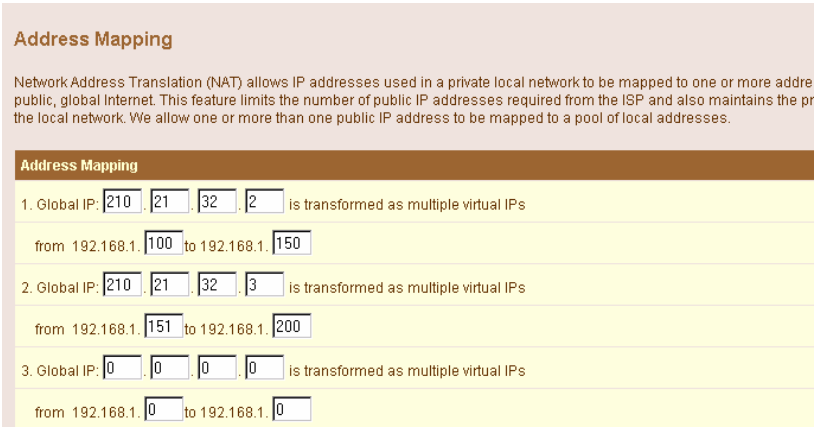
Address Mapping
Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addre
public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the pr
the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.
Address Mapping
1. Global IP: 210 . 21 . 32 . 2 is transformed as multiple virtual IPs
from 192.168.1. 100 to 192.168.1. 150
2. Global IP: 210 . 21 . 32 . 3 is transformed as multiple virtual IPs
from 192.168.1. 151 to 192.168.1. 200
3. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.1. 0 to 192.168.1. 0

Figure 5-10

5.4.2. Virtual Server

Arion 3001-4 is a NAT router. All the IP addresses coming in and going out to Arion 3001-4 can be converted between public and private IP addresses. You can configure the Arion 3001-4 as a virtual server so that remote users accessing services such as the Web or FTP at your local sites via public IP address can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP), the Arion 3001-4 redirects the external service request to the appropriate server. After entering parameters for some application, you must press "Add" button to confirm this setting. In the other way, you also can press "Clean" button to clean all fields and ready for another parameter retrying.

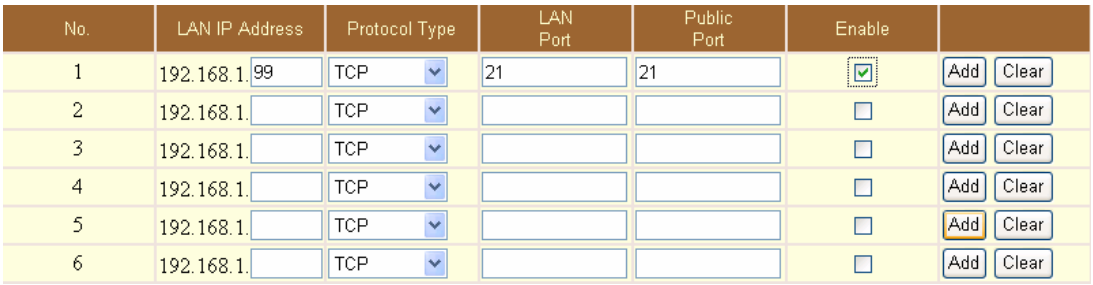

Figure 5-11

Some of the popular applications and protocol/port numbers mapping are defined below:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Table 5-1

5.4.3. Special Application

Some applications require multiple connections, such as Internet gaming and video conferencing. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

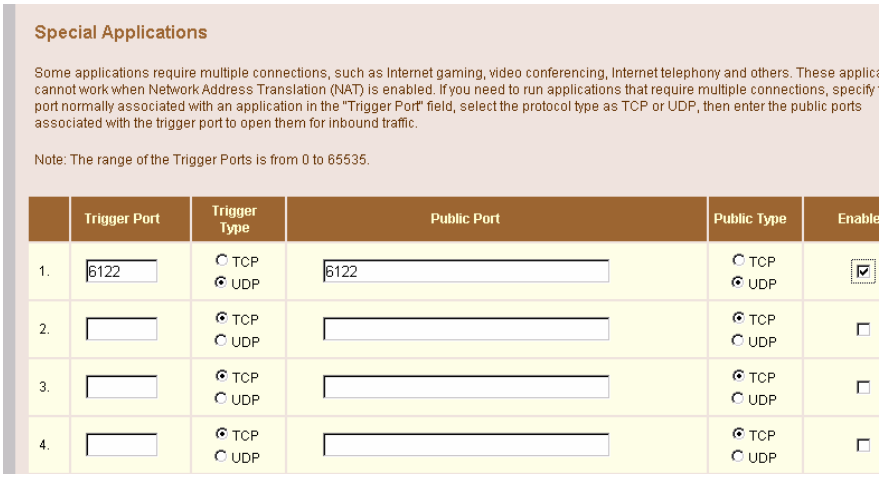
Special Applications
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applica
cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify
port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports
associated with the trigger port to open them for inbound traffic.
Note: The range of the Trigger Ports is from 0 to 65535.
Trigger Port
Trigger Type
Public Port
Public Type
Enable
1. 6122 TCP UDP 6122 TCP UDP
2. TCP UDP TCP UDP
3. TCP UDP TCP UDP
4. TCP UDP TCP UDP

Figure 5-12

Some of the applications are listed below:

Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624, 28800	UDP	MSN Game Zone
2	28800	UDP	2300-2400, 47624, 28800	TCP	MSN Game Zone
3	6112	UDP	6112	UDP	Battle.net

Table 5-2

5.5. Firewall

The Arion 3001-4 provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, by defending against a wide array of common attacks. When the firewall is enabled, extra checking will be performed for each of the packets passing through the device. However, this extra checking will also affect the performance of the device, so it should be used on an as-needed basis. To enable the firewall feature, select <Enable> from firewall page. By default, Firewall is not selected.

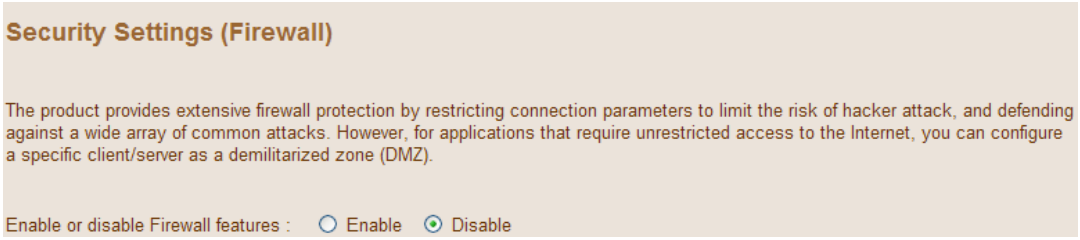
Security Settings (Firewall)
The product provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).
Enable or disable Firewall features :
Enable
Disable

Figure 5-13

5.5.1. Access Control

Access Control allows you to block specific PCs on your network from gaining access to the Internet. You can block PCs based on either the IP address or the MAC address. When the firewall is enabled, Access Control will be enabled automatically. You can disable filtering feature manually. When Access Control is enabled, all the packets will be allowed by default and you can use the <Normal Filtering Table> and the <MAC Filtering Table> to filter out disallowed traffic.

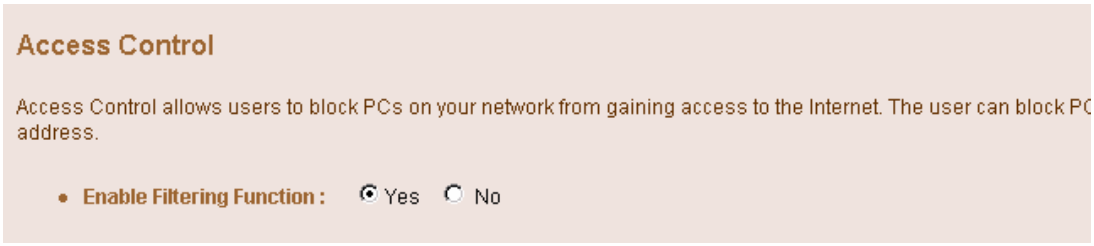
Access Control
Access Control allows users to block PCs on your network from gaining access to the Internet. The user can block PC
address.
Enable Filtering Function :
Yes
No

Figure 5-14

Normal Filtering Table

You can press <Add PC> to edit packet filtering rules.

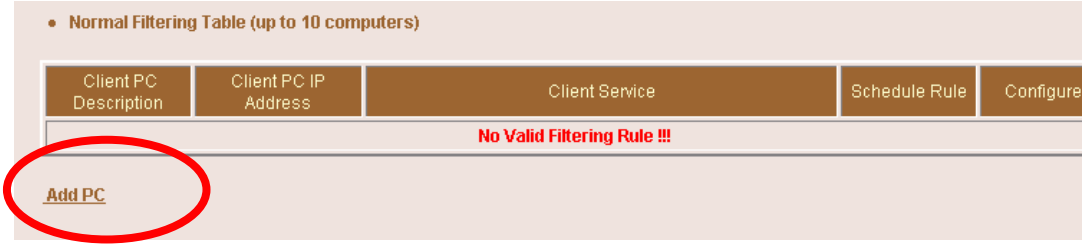

Figure 5-15

When you select <Add PC>, the following <Access Control Add PC> page will show up:

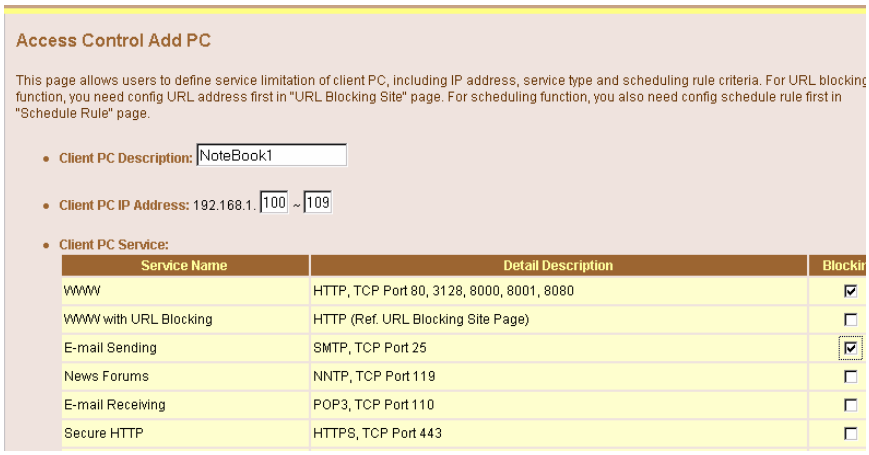
Access Control Add PC
This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need config URL address first in "URL Blocking Site" page. For scheduling function, you also need config schedule rule first in "Schedule Rule" page.
Client PC Description: NoteBook1
Client PC IP Address: 192.168.1. 100 ~ 109
Client PC Service:
Service Name
Detail Description
Blockin
WWW
HTTP, TCP Port 80, 3128, 8000, 8001, 8080
WWW with URL Blocking
HTTP (Ref. URL Blocking Site Page)
E-mail Sending
SMTP, TCP Port 25
News Forums
NNTP, TCP Port 119
E-mail Receiving
POP3, TCP Port 110
Secure HTTP
HTTPS, TCP Port 443

Figure 5-16

This page allows you to define service limitations of a client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you will need to configure the URL address first in "URL Blocking Site" page. For scheduling function, you will also need to configure schedule rule first in the "Schedule Rule" page.

As shown above, you will need to enter the Client PC Description (e.g. NoteBook1), and it's associated IP address (192.168.1.100), then select the service name <WWW> and <E-mail Sending>, and then press <OK>. The following page will then be displayed. In the example below, the PC with IP address 192.168.1.100 will not be able to use WWW or send e-mail. The Arion 3001-4 supports up to 32 filtering rules.

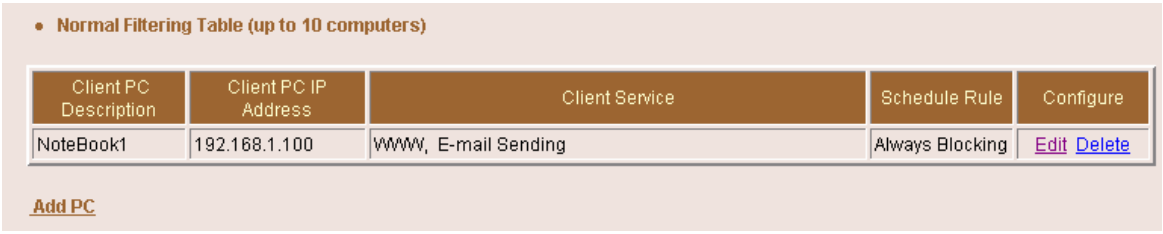

Figure 5-17

MAC Filtering Table

You can enter up to 32 MAC addresses. The PCs with these MAC addresses will not be permitted to access Internet.

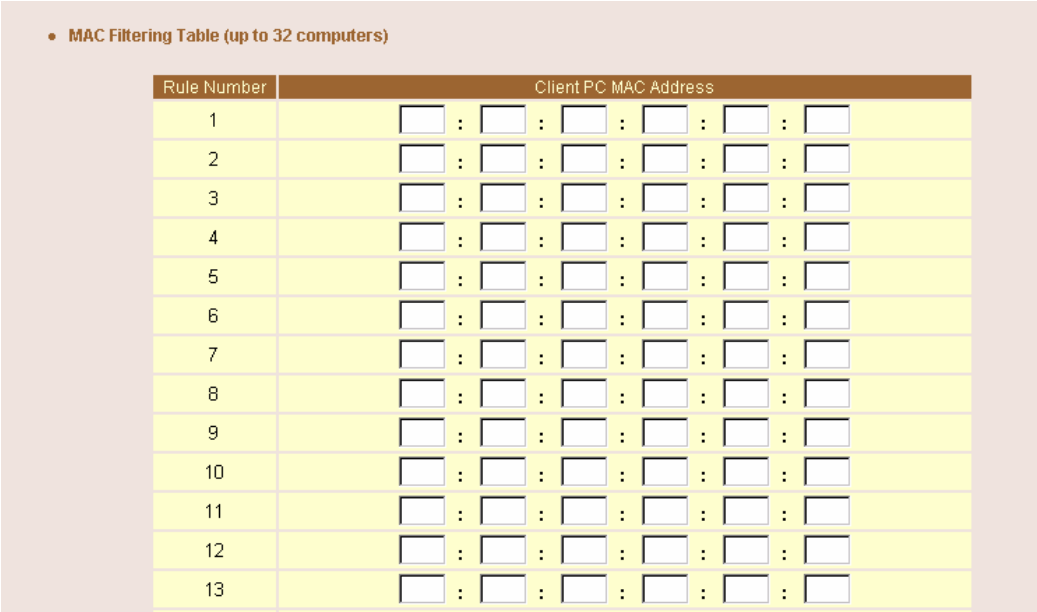

Figure 5-18

5.5.2. URL Blocking

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

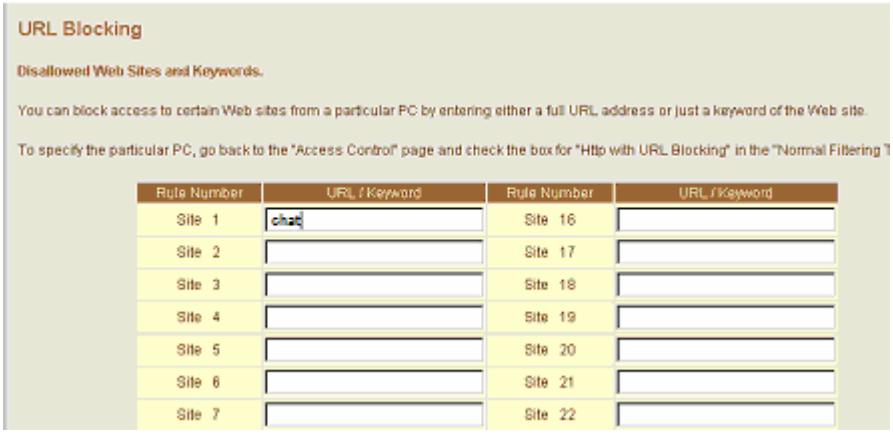
URL Blocking
Disallowed Web Sites and Keywords.
You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.
To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering
Rule Number
URL / Keyword
Rule Number
URL / Keyword
Site 1
chat
Site 16
Site 2
Site 17
Site 3
Site 18
Site 4
Site 19
Site 5
Site 20
Site 6
Site 21
Site 7
Site 22

Figure 5-19

As shown above, when the string "chat" is entered into the URL Blocking page, the PCs connected to the Arion 3001-4 will not be able to access any web-site that contains "chat" in its URL address.

5.5.3. Schedule Rule

This page allows you to define a schedule rule for use in <Access Control> page. If you press the <Add Schedule Rule>, you will be required to enter a start time and an End time. This defined schedule rule will be used under <Access Control Add PC>.

Figure 5-20

As shown above, for the schedule rule called "Office Hour", the active time period is Monday to Friday, 9:00 am to 5:00 pm. After pressing <OK>, the following page will show up:

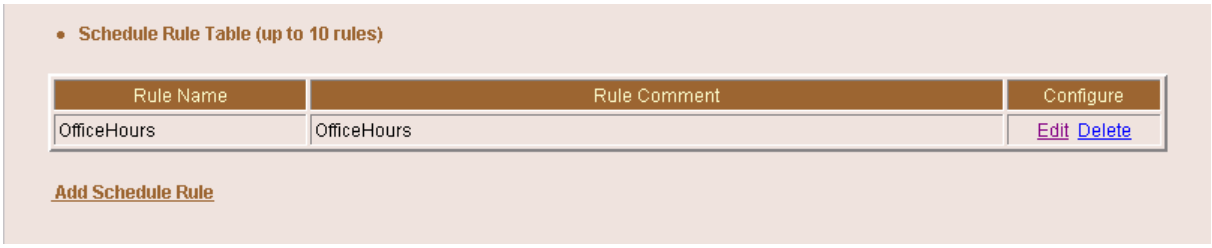

Figure 5-201

Then when we go to <Access Control> page, select <Add PC>, in the bottom of the page <Access Control Add PC>, the scheduling rule will show "Office Hour", as shown below:

Figure 5-212

If we setup the PC of finance department in our company (IP address 192.168.1.100 to 192.168.1.130) can not access the Internet during office hours, then in <Access Control> page, we will see the following page:

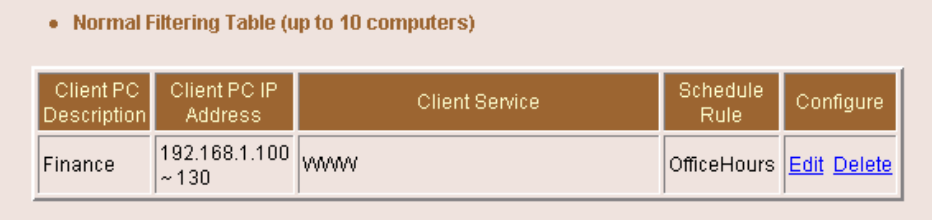

Figure 5-223

5.5.4. Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, specific packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different attack types that are using dynamic port numbers.

This product's firewall can block common hacker attacks, including:

- IP Spoofing,
- IP with zero length,
- IP With Option,
- Too Short ICMP,
- Too Short TCP,
- Too Short UDP,
- Tiny Fragment Attack,
- NewTear Attack,
- Smurf Attack,
- Land Attack,
- Ping of Death,
- UDP Loop Attack,
- Tear Drop Attack,
- Snork Attack,
- Winnuke Attack,
- Bonk Attack,
- ASCEND Probe Attack,
- Boink Attack,
- SYN Drop Attack,
- Empty Fragment Attack,
- Oshare Attack,
- TCP null scan,
- TCP Xmas scan,
- RIP defect,
- ICMP defect,
- TCP SYN flood,
- UDP flood and Fragmentation Flood.

Intrusion Detection Features:

SPI and Anti-DoS Firewall Protection	Activate SPI and Anti-DoS protection
RIP Defect	Reject the RIP packets from WAN
Discard PING from WAN	Reject all the PING request to the WAN port

Table 5-3

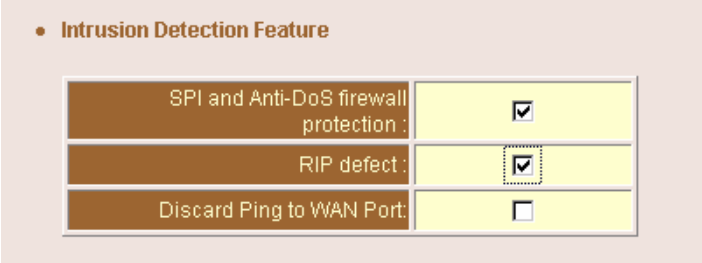

Figure 5-234

When a hacker tries to attack, the Arion 3001-4 can send e-mail alert to the specified person. You will be required to enter the related e-mail information, such as e-mail address and SMTP server. Some e-mail service providers require you to also enter POP3 information when trying to send e-mail. In this case, you will have to enter the POP3 server, user name and password.

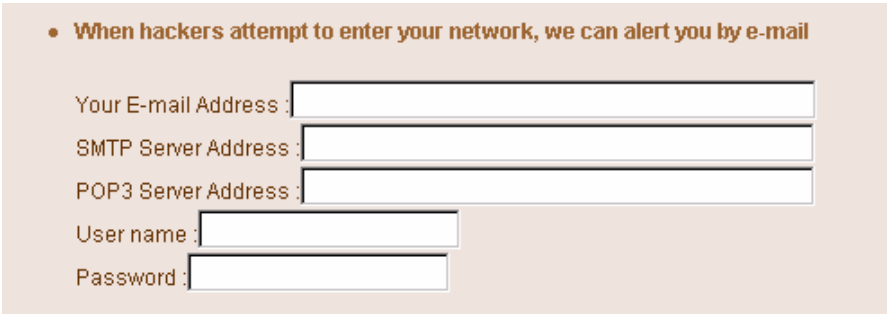
When hackers attempt to enter your network, we can alert you by e-mail
Your E-mail Address :
SMTP Server Address :
POP3 Server Address :
User name :
Password :

Figure 5-245

5.5.5. DMZ

A DeMilitarized Zone (DMZ) can expose a selected PC to the Internet, while still keeping other PCs protected. This feature could be required if an application running on that PC needs direct access from the Internet, and/or if the ports that need to be opened for inbound requests cannot be predicted.

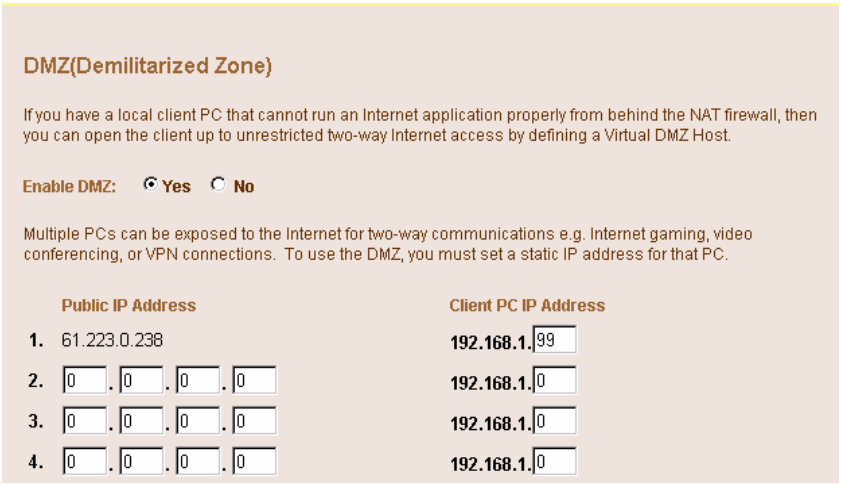
DMZ(Demilitarized Zone)
If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.
Enable DMZ: Yes No
Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.
Public IP Address
Client PC IP Address
1. 61.223.0.238 192.168.1.99
2. 0.0.0.0 192.168.1.0
3. 0.0.0.0 192.168.1.0
4. 0.0.0.0 192.168.1.0

Figure 5-256

6. UPnP

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all types, intelligent appliances, and wireless devices. UPnP enables seamless connectivity between the router and various networked devices at home.

For example, if user wants to use Windows XP Messenger application, this feature should be enabled.

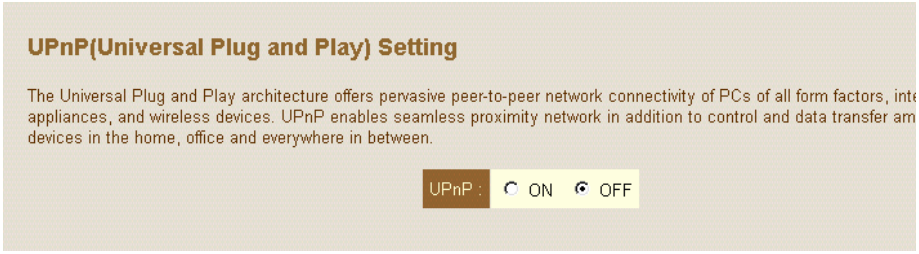
UPnP(Universal Plug and Play) Setting
The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, inte
appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer am
devices in the home, office and everywhere in between.
UPnP :
ON
OFF

Figure 6-1

7. DDNS

Dynamic DNS provides users on the Internet a method to tie their domain name to a temporary IP address automatically, by changing the DDNS records every time your IP address changes.

Two DDNS providers are supported, TZO.com and DynDNS.org. You must apply for DDNS service to get a Key from the DDNS provider and then enable the DDNS service using the following page.

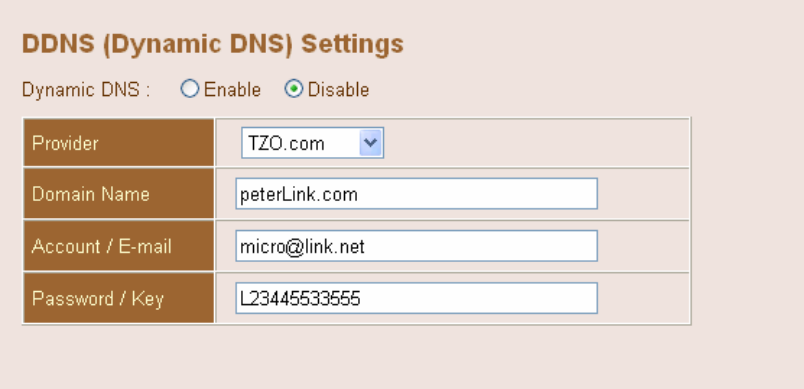

Figure 7-1

8. Tools

The tools feature provided with the Arion 3001-4 includes configuration tools – save /restore configuration and restore to factory defaults, system log, firmware upgrade and reset. The main page is shown below.

8.1. Configuration Tools

The configuration tools includes backup, restore and restore to factory defaults. The "Backup" tool saves the Arion 3001-4's current configuration to a file named "backup_config.bin" on your PC. You can then use "Restore" tool to restore the saved configuration to the Arion 3001-4. The "Reset to Factory Defaults" tool will force the configuration of Arion 3001-4 back to the original factory setting and perform a power reset.

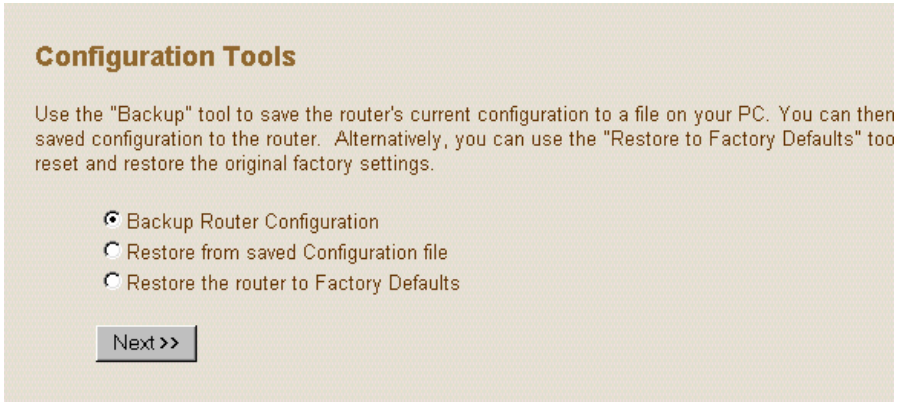
Configuration Tools
Use the "Backup" tool to save the router's current configuration to a file on your PC. You can then
saved configuration to the router. Alternatively, you can use the "Restore to Factory Defaults" too
reset and restore the original factory settings.
Backup Router Configuration
Restore from saved Configuration file
Restore the router to Factory Defaults
Next >>

Figure 8-1

8.2. Firmware Upgrade

The firmware upgrade tool allows you to upgrade the Arion 3001-4 system's firmware. You need to download the image file to your local PC first, and select the target file to upload. The Arion 3001-4 has 3 items target, one for core firmware, one for the user interface, and another one is Voice file. If you have more then one item to be upgraded, please upgrade User Interface first

Firmware Upgrade
This tool allows you to upgrade the router firmware using a file provided by the manufacturer.
Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process.
Upgrade Target :
Firmware and UI
Firmware File :
瀏覽...

Figure 8-2

8.3. Reset

In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the

APPLY button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking

9. Status

These status pages display the status of the system, including the connection status of the interfaces, firmware and hardware version numbers, system log and DHCP client information. The Status and Information page below, shows MAC addresses, and hardware/software versions.

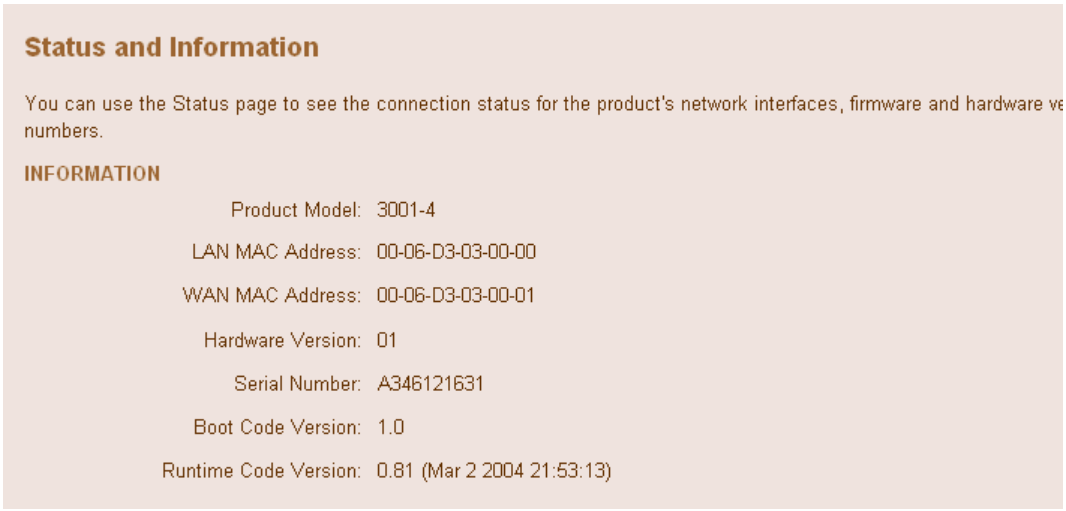
Status and Information
You can use the Status page to see the connection status for the product's network interfaces, firmware and hardware ve
numbers.
INFORMATION
Product Model: 3001-4
LAN MAC Address: 00-06-D3-03-00-00
WAN MAC Address: 00-06-D3-03-00-01
Hardware Version: 01
Serial Number: A346121631
Boot Code Version: 1.0
Runtime Code Version: 0.81 (Mar 2 2004 21:53:13)

Figure 9-1

9.1. Internet Connection

The Internet Connection page displays the status of the Internet Connection, including the connection status of the Internet interfaces, WAN port IP, Subnet Mask, Gateway IP and Primary/ Secondary DNS IP.

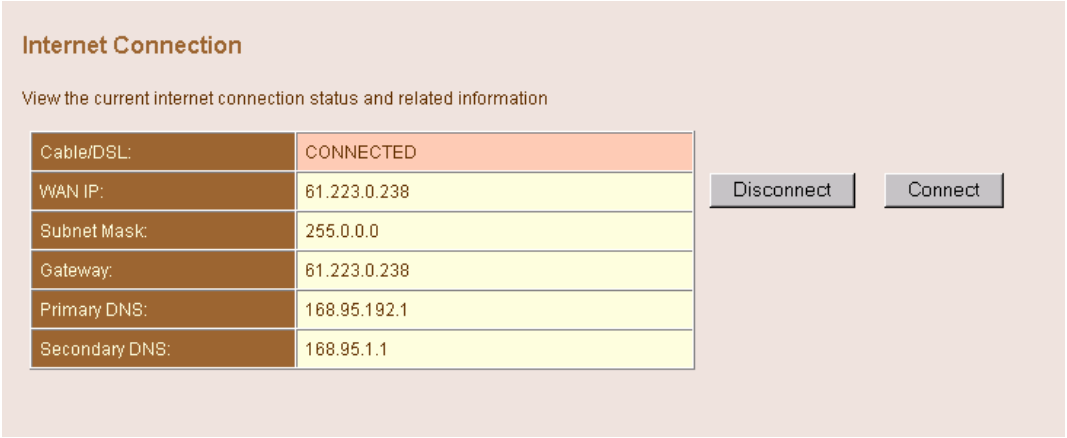

Figure 9-2

When WAN port setting is dynamic IP, user can use <Disconnect> and <Connect> to release and update WAN port IP

9.2. Device Status

The Device Status page displays the current setting of this device, including IP address, Subnet mask, DHCP server, Firewall and UPnP.

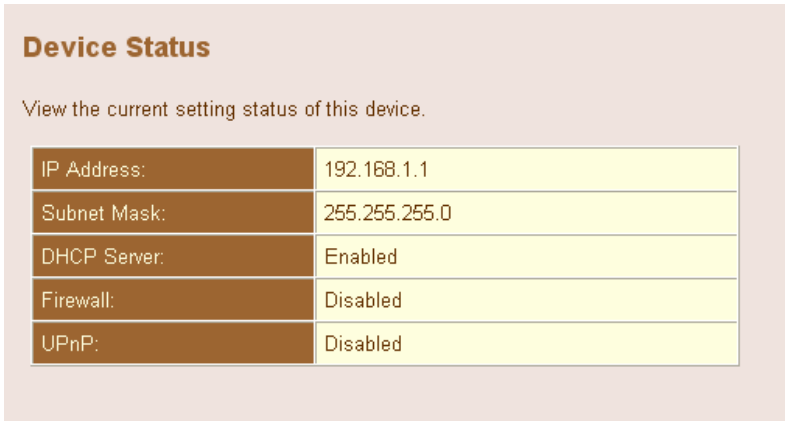

Figure 9-3

9.3. Security Log

This page provides the system security log record when the Arion 3001-4 boots, including user login/logout, hacker attack, PPPoE connection, NTP connection, Get IP from DHCP, etc…

These records can be saved to host PC. User also can clear all security records in Security log window and press <Refresh> to update current security records.

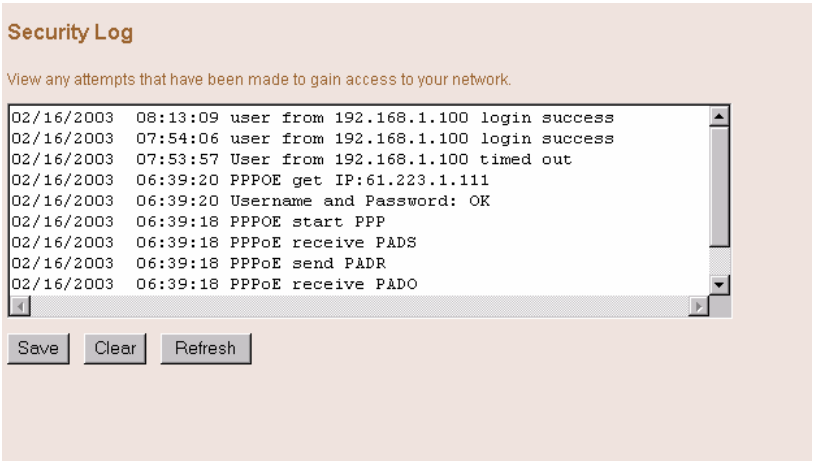
Security Log
View any attempts that have been made to gain access to your network.
02/16/2003 08:13:09 user from 192.168.1.100 login success
02/16/2003 07:54:06 user from 192.168.1.100 login success
02/16/2003 07:53:57 User from 192.168.1.100 timed out
02/16/2003 06:39:20 PPPOE get IP:61.223.1.111
02/16/2003 06:39:20 Username and Password: OK
02/16/2003 06:39:18 PPPOE start PPP
02/16/2003 06:39:18 PPPoE receive PADS
02/16/2003 06:39:18 PPPoE send PADR
02/16/2003 06:39:18 PPPoE receive PADO
Save
Clear
Refresh

Figure 9-4

9.4. DHCP Client Log

The DHCP Client Log page displays the IP addresses assigned to PCs in your network. You can press the <Refresh> button to update current IP allocation records.

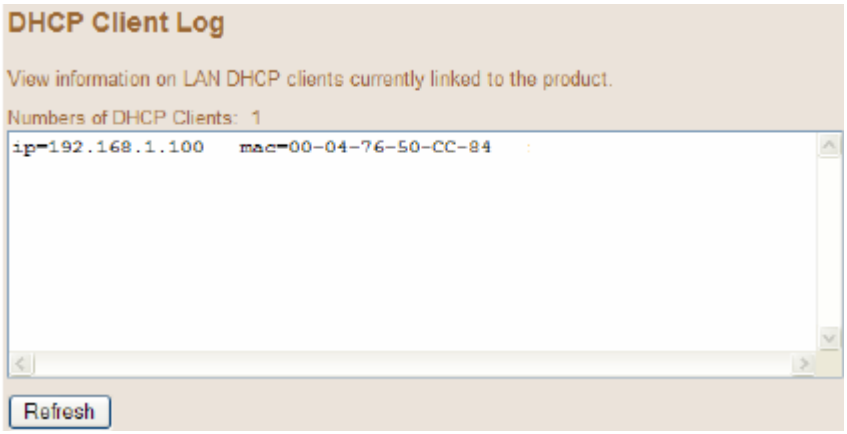
DHCP Client Log
View information on LAN DHCP clients currently linked to the product.
Numbers of DHCP Clients: 1
ip=192.168.1.100 mac=00-04-76-50-CC-84
Refresh

Figure 9-5

9.5. VoIP Status

This page displays the gateway status, including Port type, port Status, time information of each call and Destination. This page also displays gatekeeper status. You must make sure the gatekeeper is registered.

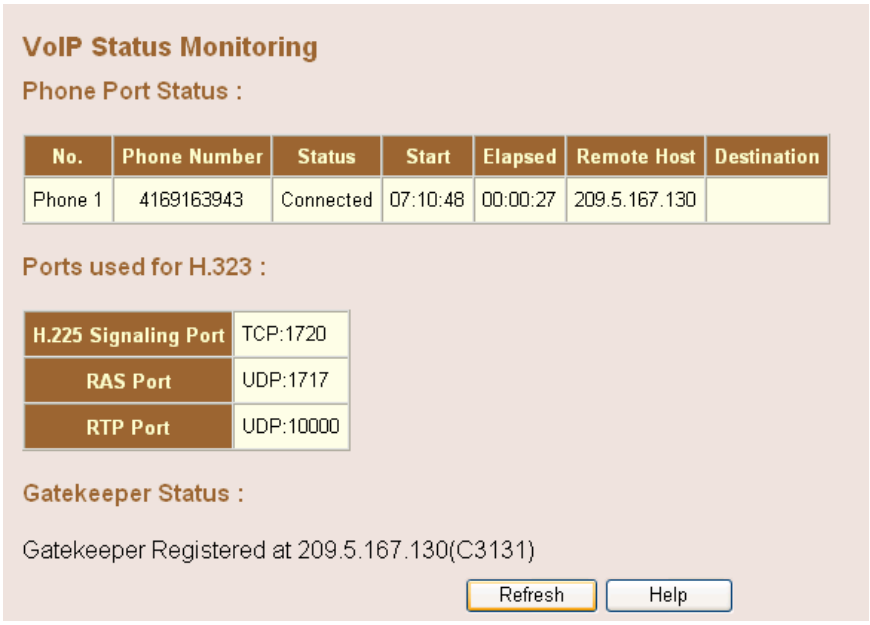

Figure 9-6

You can press the <Refresh> button to update the current VoIP status.

Glossary

ITSP: Short for Internet Telephony Service Provider, which is a general term for the organization which provides the Internet Telephony service to the general public.

POTS: Short for Plain Old Telephone Service, which refers to the standard telephone service that most homes use. In contrast, telephone services based on high-speed, digital communications lines, such as ISDN and FDDI, are not POTS. The main distinctions between POTS and non-POTS services are speed and bandwidth. POTS is generally restricted to about 52 Kbps (52,000 bits per second).

PSTN: The POTS network is also called the Public Switched Telephone Network (PSTN).

PBX: Short for Private Branch eXchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

FXO: Short for Foreign Exchange Office interface, which is used to connect to the central office of the PSTN to receive signals from PSTN.

FXS: Short for Foreign Exchange Station interface, which is used to connect to the telephone set or PBX, it provides ringing back, dial signal to the telephone devices.

H.323: H.323 is an International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

Gatekeeper: The gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper. The gatekeeper is an H.323 entity on the LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper may provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.

H.245: H.323 is an International Telecommunication Union (ITU-T) standard that defines the control functions of the network multimedia communication, such as the agreement of the mutual communication capability, the establishment of the voice and video channel, etc. It could be used in H.323 and H.324.

E.164: Phone number: The international standard telephone number. It starts with the country code, area code and local phone number.